CLAIMS

Sub a8

1. An improved personal device to be connected to a terminal for establishing a trustworthy connection between a user via said device and said terminal which is connected to and authenticatable by at least one server, the improvement comprising at least one storage component for storing predetermined authentication information (vec) communicatable to the terminal for said terminal to create an authenticity output message.

2. An improved personal device to be connected to a terminal for establishing a trustworthy connection between a user via said device and said terminal which is connected to and authenticatable by at least one server, the improvement comprising at least one device authentication component for said device to authenticate itself to the terminal.

3. An improved personal device to be connected to a terminal for establishing a trustworthy connection between a user via said device and said terminal which is connected to and authenticatable by at least one server, the improvement comprising messaging component for requesting user authentication information from the user and a comparison component for verifying the authenticity of the user authentication information.

4. The improved personal device, according to claim 1, wherein the authenticity output message (m_o) comprises at least one of visible, audible and tactile information.

5. The improved personal device, according to claim 1, wherein the authenticity output message (m_o) comprises at least one value for lookup in a table stored in the terminal.

6. A terminal for establishing a trustworthy connection between a user and a server, the terminal comprising:

a device input component for input of a user device;

a communication component for establishing and conducting communications with a server and for receiving at least one authenticity output message from said server; and

at least one message output component for outputting the at least one authenticity output message to the user.

7. The terminal according to claim 6 further comprising at least one user input interface component for receiving user input.

8. The terminal according to claim 6 further comprising a stored lookup table which is accessible via the authenticity output message.

9. A server being equipped for establishing a trustworthy connection between a user and a terminal via a user input device comprising:

a communication component for establishing and conducting communications with the terminal;

receiver means for receiving at least one authentication request from said terminal;

at least one authentication component for verifying the authenticity of the terminal; and

a message generation component for generating at least one authenticity output message for delivery to said user at said terminal.

10. The server according to claim 9 further comprising a session key creation component for creating a session key to be communicated to said terminal.

11. The server according to claim 9 further comprising at least one storage location for storing at least one user-specific authenticity output message and wherein said message generation component accesses the stored at least one user-specific authenticity output message for display to the user at said terminal.

12. A method for establishing a trustworthy connection between a user via said personal device and a terminal which is connected to and authenticatable by at least one server which is authenticatable by said device, comprising:

said server authenticating said terminal;

establishing a first authenticated trusted connection upon success of said authenticating;

said server authenticating itself to said device;

establishing a second trusted connection between said server and said device; and

said server providing a terminal authenticity message via said established second trusted connection confirming the established authenticity of said terminal;

13. The method according to claim 12 further comprising communicating said terminal authenticity message to said user.

14. The method according to claim 13 wherein said communicating comprises displaying said message by said device.

15. The method according to claim 13 wherein said communicating comprises displaying said message by said terminal.

16. The method according to claim 12 wherein said providing a terminal authenticity message comprises accessing at least one stored user-specific message.

17. The method according to claim 12 wherein said providing a terminal authenticity message comprises exchanging a predetermined set of messages with said user.

18. The method according to claim 15 wherein stored predetermined authentication information (vec) is communicated from the device to the terminal for creating there an authenticity output message (m_o).

19. The method, according to claim 12 further comprising the device authenticating itself to the terminal.

20. The method according to claim 12 further comprising the device requesting that the user authenticate himself.

21. The method according to claim 14 wherein the device outputs the terminal authenticity message including at least one of visible, audible and tactile information.

22. The method according to claim 15 wherein the terminal outputs the terminal authenticity message including at least one of visible, audible and tactile information

23. The method according to claim 21 wherein the message is output only partially by the device, according to a preselection by the user.

24. The method according to claim 21 wherein the message is output only partially by the terminal according to a preselection by the user

25. The method according to claim 12 further comprising authenticating the device to the server.

26. The method according to claim 12 further comprising authenticating the user.

27. A method for a server to establish a trustworthy connection to a user from a terminal comprising the steps of:

receiving input from a terminal at which said user is accessing said server;

authenticating the terminal; and

generating a terminal authenticity message to said user.

28. The method according to claim 27 wherein said generating comprises accessing at least one stored message.

29. The method according to claim 28 wherein said generating comprises performing an exchange of messages with said user according to a stored authenticity message.

30. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for a server to establish a trustworthy connection with a user via a terminal, said method steps comprising:

receiving input from a terminal at which said user is accessing said server;

authenticating the terminal; and

generating a terminal authenticity message to said user.